UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/715,350	11/17/2000	David Montgomery	0500.0003231	6328

23418 7590 01/13/2005

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/715,350	MONTGOMERY, DAVID	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communicati n appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,12-17,19-21,24-33,35 and 37-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,12-17,19-21,24-33,35 and 37-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 8/9/04 was received and considered.

2. Claims 1-7, 12-17, 19-21, 24-33, 35 & 37-46 are pending.

Response to Arguments

3. The indicated allowability of claims 8, 11, 22 & 34 is withdrawn in view of further consideration (see rejections below). Accordingly, this Office Action is non-final.

4. Applicant's response (p. 14, ¶4) argues that claim 1 is statutory because the obtaining of cross certificates "may include, for example, reading cross certificate information from memory, requesting information from a repository, or any other suitable operation." However, claim 1 lacks recitation of a memory or any specific hardware required to perform the method. Therefore the method of claim 1, as recited, is not tangibly embodied.

5. Applicant's response (p. 14, ¶5 – p. 15, ¶1) regarding claim 16's inclusion of a "generator" is persuasive. The rejection of claims 16-25 under 35 U.S.C. §101 set forth in the previous Office Action is withdrawn.

6. In light of applicant's response (p. 15, ¶2) and amendment to claim 6, the objection of claim 6, set forth in the previous Office Action is withdrawn.

7. Applicant's response (p. 15, ¶3) argues that the cited portion of NAI fails to teach "creating a signed certificate set identifying certificate issuing units that are trusted by an anchor certificate issuing unit based on a cross certificate" and "collecting certificates for a community of interest". This is interpreted as equivalent to "creating a set of signed certificates". Applicant is directed to p. 33, ¶1-2 of NAI where the key ring is a signed set of public keys that are

certified by the anchor. Further, the key ring is encrypted and a signature is simply an encryption to be later verified. The certificates for a community are collected (either signed by the anchor or other, such as Alice) and added to a key ring/certificate set.

8. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "the set must include two or more certificate issuing units determined to be trusted by an anchor certificate issuing unit") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claims recite "a signed certificate set identifying certificate issuing units", rather than "two or more". For example, in the NAI reference, the author refers to "the people he trusts", but standard interpretation does not require that "he" trust more than 1 person, but rather 0 or more.

9. Applicant's response (p. 15, last ¶ - p. 16, ¶1) argues that the NAI reference fails to teach collecting certificates identified in a cross certificate or identified in another certificate or creating a signed set of information that identifies certificate issuing units in a group. NAI discloses the collection of certificates identified in a certificate (when Alice signs another user's key, which creates a certificate, the other user's key appears as valid on the anchor's keyring) and creating a signed set of information/keyring that identifies certificate issuing units in a group (p. 33, ¶1-2), but the certificate being specifically a "cross certificate" is taught in the Menezes reference.

10. Applicant's response (p. 16, ¶2) argues that the Menezes reference fails to teach "the collecting of cross certificates for an anchor CA" and "creating any kind of a signed certificate

set that identifies certificate issuing units determined to be trusted by the anchor certificate issuing units as required by the claims." The collection is disclosed in NAI and is described above. The creating a signed certificate set/keyring determined to be trusted is also taught in NAI, as described above.

11. Applicant's response (p. 16, ¶3) argues that claims 2, 27 & 31 are believed to be allowable because there is no teaching or suggested of a signed certificate set which contains information relating to multiple trusted CA's. However, NAI teaches the collecting of certificates from introducers the anchor trusts (CA's) and further collecting certificates they sign. All participants in the PGP system can be certificate issuers. Further, the applicant is reminded that the claims do not recite "CA" or "certificate authority".

12. Applicant's response (p. 16, ¶4) argues that NAI fails to teach the "creation of a signed certificate set". Applicant is directed to the keyring of NAI (p. 33, ¶1-2).

Claim Rejections - 35 USC § 101

13. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

14. Claims 1-7 & 12-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 presents a method of issuing certificates; the claim language is related to a mathematical operation not tangibly embodied. Claim 16 presents an apparatus performing the method of claim 1. Claims 2-7 & 12-15 are rejected based on their dependence upon claim 1.

15. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 (nonstatutory) above are further rejected as set forth below in anticipation of the applicant amending these claims to place them within the four statutory classes of invention.

Claim Rejections - 35 USC § 112

16. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

17. Claims 1-7, 12-17, 19-21, 24-33, 35 & 37-46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1-7, 12-17, 19-21, 24-33, 35 & 37-46, "signed certificate set" can be interpreted as equivalent to "a set of certificates that is signed" or "a set of signed certificates" and the claims are therefore vague and indefinite.

Regarding claim 25, the claim depends on a canceled claim and is therefore indefinite.

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 1-7, 12-13, 16-17, 19-21, 24-33, 35, 37-38, 41, 43 & 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over "An Introduction to Cryptography" by Network

Associates, Inc. (NAI) in view of Handbook of Applied Cryptography by Menezes et al. (Menezes).

Regarding claims 1, 16, 30 & 41, NAI discloses collecting at least one certificate associated with an anchor certificate issuing unit/home user (page 33, ¶1-2) and obtaining at least one (one) certificate issuing unit/(user validated by trusted introducer Alice) public key and an associated unique identifier (certificate) (page 33, ¶2) for a certified certificate issuing unit/Alice identified by the at least one certificate (validated Alice's key/certificate), and creating a signed certificate set/keyring (page 33, ¶1, page 18, ¶3 & page 28, ¶2) identifying the certificate issuing units/(users validated by trusted introducer Alice) determined to be trusted by the anchor certificate issuing unit/home user, based on the at least one certificate/Alice's certificate wherein the signed certificate set includes at least the unique identifier and the public key of each trusted certificate issuing unit/(users validated by trusted introducer Alice) (page 33, ¶1). NAI lacks a cross certificate. However, Menezes teaches that a cross-certificate is simply a certificate created by one certification authority, certifying the public key of another CA (§13.6.1, def. 13.39). NAI discloses that in PGP, users act as certification authorities (page 32, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to obtain a cross-certificate and use the information in that rather than the certificate, as disclosed by NAI. One of ordinary skill in the art would have been motivated to perform such a modification because each user acts as a certificate authority (NAI, page 32, ¶3) and cross-certificates are used by one CA to certify another, as taught by Menezes (§13.6.1, def. 13.39).

Regarding claims 2, 27 & 31, NAI, as modified above, discloses generating a signed certificate set revocation list/certificate revocation list containing at least an identifier of at least one signed certificate set that has been revoked (page 34).

Regarding claim 3, NAI, as modified above, lacks specifically obtaining cross certificates by obtaining chained cross certificates from a plurality of certificate issuing units. However, NAI teaches that if a direct trust path is not found, a path of chained certificates can be followed to establish a trust relationship between entities (page 31, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to obtain cross certificates by obtaining chained cross certificates from a plurality of certificate issuing units. One of ordinary skill in the art would have been motivated to perform such a modification to establish a trust relationship where a direct trust path did not exists, as taught by NAI (page 31, ¶1).

Regarding claims 4, 19, 28 & 32, as modified above and as best understood, NAI discloses publishing the signed certificate set of certificate issuing units certificates/CRL, accessible by a plurality of different clients (page 28, ¶2 & page 34, ¶5).

Regarding claims 5 & 37, as modified above, NAI discloses publishing the signed certificate set of certificate issuing units certificates/CRL accessible by a plurality of different clients (page 28, ¶2 & page 34, ¶5) and distributing the signed certificate/CRL set to client units/users (page 34, ¶5-6). Note that publishing a set of certificates, each containing an identifier, is substantially equivalent to publishing a certificate-issuing unit.

Regarding claims 6 & 20, NAI, as modified above, discloses collecting cross certificates from a data repository/keyring associated with the anchor CA/the user (page 33, ¶2).

Regarding claims 7, 21 & 33, NAI, as modified above, discloses that the signed certificate set of certificate issuing units/keyring is digitally signed (page 18, ¶3), which inherently provides a trusted cross certificate (page 28, ¶1-4 & page 68) (a user A's signature on another user B's certificate indicates trust – a user C who trusts A will then trust B) (page 28).

Regarding claims 12, 24, 29 & 35, NAI, as modified above, discloses creating a plurality of signed certificate sets/keyrings on a per anchor certificate issuing unit/user basis (page 18, ¶3) where each signed certificate set contains at least: a list of unique identifiers and associated public keys (page 21) of each certificate issuing unit trusted by an anchor certificate issuing unit/user (page 33, ¶1-2), and publishing each signed certificate set/public keyring wherein each published signed certificate set is accessible by a plurality of different client units/users (page 28, ¶2 & page 18, ¶3).

Regarding claims 13 & 25, as best understood, NAI, as modified above, discloses validating a digital signature on each cross certificate (Alice) and including only validated certificate issuing units/CA's that have valid certificates (validated certificate appears on your (user's) keyring) (page 33, ¶1-2).

Regarding claim 17, NAI discloses the signed certificate set/keyring generator/user generating and publishing a signed certificate set revocation list/CRL containing at least an identifier (certificate) of at least one signed certificate set that has been revoked (page 34).

Regarding claims 26, NAI discloses a signed certificate set/keyring generator/user collecting at least one certificate associated with an anchor certificate issuing unit/home user (page 33, ¶1-2) and obtaining at least one (one) certificate issuing unit/(user validated by trusted introducer Alice) public key and an associated unique identifier (certificate) (page 33, ¶2) for a

certified certificate issuing unit/Alice identified by the at least one certificate (validated Alice's key/certificate), and creating a signed certificate set/keyring (page 33, ¶1, page 18, ¶3 & page 28, ¶2) identifying the certificate issuing units/(users validated by trusted introducer Alice) determined to be trusted by the anchor certificate issuing unit/home user, based on the at least one certificate/Alice's certificate wherein the signed certificate set includes at least the unique identifier and the public key of each trusted certificate issuing unit/(users validated by trusted introducer Alice) (page 33, ¶1). NAI further discloses at least one client unit/user in operative communication with the signed certificate set generator/user operative to access the signed certificate set/keyring to determine whether a received message is from a trusted source based on the signed certificate set/keyring (page 28, ¶2). NAI lacks a cross certificate. However, Menezes teaches that a cross-certificate is simply a certificate created by one certification authority, certifying the public key of another CA (§13.6.1, def. 13.39). NAI discloses that in PGP, users act as certification authorities (page 32, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to obtain a cross-certificate and use the information in that rather than the certificate, as disclosed by NAI. One of ordinary skill in the art would have been motivated to perform such a modification because each user acts as a certificate authority (NAI, page 32, ¶3) and cross-certificates are used by one CA to certify another, as taught by Menezes (§13.6.1, def. 13.39).

Regarding claims 38, 43 & 45, NAI lacks adding at least a validity period, serial number, set extension or policy identifier. However, Menezes teaches that common forms of additional information are added to certificates, such as a serial number to identify the certificate (§13.4.2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to include a serial number in the signed certificate set. One of ordinary skill in the art would have been motivated to perform such a modification to identify the certificate set, as taught by Menezes (§13.4.2).

20. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over NAI in view of Menezes, as applied to claim 1 above, in further view of U.S. Patent 6,321,333 to Murray. NAI, as modified above, discloses validating an end-entity/user certificate using the public key of the certificate issuing authority/CA associated with the certificate (page 30, ¶1) and discloses that to verify a user without previous contact, one can use the trust relationship already established with the user's CA (pages 30-32), but lacks caching a copy of the signed certificate set/keyring and validating and end-entity certificate by seeing if the certificate issuing entity/CA associated with the end-entity is on the cached signed certificate set/keyring and using the public key of that certificate issuing entity to validate the end-entity certificate. However, Murray teaches that certificate validation is more efficient when a certificate cache is employed where the user first checks to see if the certificate presented is in the cache and determines that it is valid if it is in the cache (col. 2, lines 13-34). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ a certificate cache to cache the keyring/certificate set to validate that the end-entity's CA's certificate is in the cache. One of ordinary skill in the art would have been motivated to perform such a modification to increase efficiency, as taught by Murray (col. 2, lines 13-34).

21. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over NAI in view of Menezes, as applied to claim 1 above, in further view of "Federal Bridge CA Concept" by Burr, 5/4/2000. NAI, as modified above, lacks applying policy constraints including placing identifiers of those policy constraints in the signed set/keyring. However, Burr teaches that certificate policies enable a user to describe a level of assurance to a certificate and intended uses of the certificate (page 32). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply policy constraints including placing identifiers/levels of assurance in the signed set/keyring. One of ordinary skill in the art would have been motivated to perform such a modification to describe a level of assurance a user has in the keyring and to assert an intended use, as taught by Burr (page 32).

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
January 3, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100